LISTING OF CLAIMS

Please amend the claims as follows:

1-34 Cancelled

35. (New) A method for secure wireless communication using spread spectrum principles, comprising:

generating at least one pseudorandom number (PN) sequence;

generating at least one encryption sequence based on at least one of key and time-varying input;

combining the PN sequence with said encryption sequence to render an encrypted PN sequence; and

using the encrypted PN sequence to spread a communication signal.

36. (New) The method of Claim 35, wherein the communication signal is received from a data modulation component including a Walsh modulator.

37. (New) The method of Claim 35, wherein the encryption sequence is generated by a data encryption standard (DES) component or a triple-DES component.

38. (New) The method of Claim 37, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

39. (New) The method of Claim 38, wherein the at least one multi-bit key is periodically refreshed.

40. (New) An apparatus for secure wireless communication using spread spectrum principles, comprising:

means for generating at least one pseudorandom number (PN) sequence;

means for generating at least one encryption sequence based on at least one of key and time-varying input;

means for combining the PN sequence with said encryption sequence to render an encrypted PN sequence; and

means for using the encrypted PN sequence to spread a communication signal.

41. (New) The apparatus of Claim 40, wherein the communication signal is received from a data modulation component including a Walsh modulator.

42. (New) The apparatus of Claim 40, wherein the encryption sequence generating means comprises a data encryption standard (DES) component or a triple-DES component.

43. (New) The apparatus of Claim 42, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

44. (New) The apparatus of Claim 43, wherein the at least one multi-bit key is periodically refreshed.

45. (New) An apparatus for secure wireless communication using spread spectrum principles, comprising:

a pseudorandom number (PN) sequence configured to generate at least one PN sequence;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input and further configured to combine the PN sequence with the encryption sequence to render an encrypted PN sequence; and

a spreader configured to use the encrypted PN sequence to spread a communication signal.

46. (New) The apparatus of Claim 45, wherein the communication signal is received from a data modulation component including a Walsh modulator.

47. (New) The apparatus of Claim 45, wherein the encryption sequence generator comprises a data encryption standard (DES) component or a triple-DES component.

48. (New) The apparatus of Claim 47, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

49. (New) The apparatus of Claim 48, wherein the at least one multi-bit key is periodically refreshed.

50. (New) A processor for secure wireless communication using spread spectrum principles, said processor being configured to:

generate at least one pseudorandom number (PN) sequence;

generate at least one encryption sequence based on at least one of key and time-varying input;

combine the PN sequence with said encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to spread a communication signal.

51. (New) A computer-program product for secure wireless communication using spread spectrum principles, comprising:

a computer-readable medium comprising instructions for causing a computer to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine the PN sequence with said encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to spread a communication signal.

52. (New) A method for secure wireless communication using spread spectrum principles comprising:

generating at least one encryption sequence based on at least one of key and time-varying input;

combining a PN sequence with the encryption sequence to render an encrypted PN sequence; and

using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

53. (New) The method of Claim 52 further comprising:

sending the despread signal to a Walsh demodulator.

54. (New) The method of Claim 52, wherein the encryption sequence is generated by a data encryption standard (DES) component or a triple-DES component.

55. (New) The method of Claim 54, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

56. (New) The method of Claim 55, wherein the multi-bit key is periodically refreshed.

57. (New) The method of Claim 55, wherein the time-varying input is at least one long code state.

58. (New) An apparatus for secure wireless communication using spread spectrum principles comprising:

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input;

a PN sequence generator configured to combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

a despreader configured to use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

59. (New) The apparatus of Claim 58 further comprising:

a Walsh demodulator configured to receive a despread signal.

60 (New) The apparatus of Claim 58, wherein the encryption sequence generator comprises a data encryption standard (DES) component or a triple-DES component.

61. (New) The apparatus of Claim 60, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

62. (New) The apparatus of Claim 61, wherein the multi-bit key is periodically refreshed.

63. (New) The apparatus of Claim 61, wherein the time-varying input is at least one long code state.

64. (New) An apparatus for secure wireless communication using spread spectrum principles comprising:

means for generating at least one encryption sequence based on at least one of key and time-varying input;

means for combining a PN sequence with the encryption sequence to render an encrypted PN sequence; and

means for using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

65. (New) The apparatus of Claim 64 further comprising:

means for sending the despread signal to a Walsh demodulator.

66. (New) The apparatus of Claim 64, wherein the generating means comprises a data encryption standard (DES) component or a triple-DES component.

67. (New) The apparatus of Claim 66, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

68. (New) The apparatus of Claim 67, wherein the multi-bit key is periodically refreshed.

69. (New) The apparatus of Claim 67, wherein the time-varying input is at least one long code state.

70. (New) A processor for secure wireless communication using spread spectrum principles, said processor being configured to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

71. (New) A computer-program product for secure wireless communication using spread spectrum principles comprising:

a computer-readable medium comprising instructions for causing a computer to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.